VOLUME 71 2002

MATHEMATICS OF COMPUTATION

AMERICAN MATHEMATICAL SOCIETY

EDITED BY

Randolph E. Bank
David W. Boyd
Susanne C. Brenner
Richard P. Brent
Joe P. Buhler
Carsten Carstensen
Arjeh M. Cohen
Ronald F. A. Cools
Howard Elman
Richard S. Falk
Daniel W. Lozier
Zhi-Quan Luo
Roswitha März
Harald Niederreiter
Ricardo Horacio Nochetto
Stanley Osher
Haesun Park
Joseph E. Pasciak
Lothar Reichel
René Schoof
Igor E. Shparlinski
Chi-Wang Shu, *Managing Editor*
Frank Stenger
Denis Talay
Nico M. Temme
Lars B. Wahlbin
Joseph D. Ward
Hugh C. Williams
Jinchao Xu

PROVIDENCE, RHODE ISLAND USA

ISSN 0025-5718

Mathematics of Computation

This journal publishes research articles in computational mathematics. Areas covered include numerical analysis, with emphasis on the mathematical analysis and development of methods, computational number theory and algebra, and related fields. Table errata and reviews of books in areas related to computational mathematics are also included.

Submission information. See **Information for Authors** at the end of this issue.

Publisher Item Identifier. The Publisher Item Identifier (PII) appears at the top of the first page of each article published in this journal. This alphanumeric string of characters uniquely identifies each article and can be used for future cataloging, searching, and electronic retrieval.

Postings to the AMS website. Articles are posted to the AMS website individually after proof is returned from authors and before appearing in an issue.

Subscription information. *Mathematics of Computation* is published quarterly. Beginning in January 1996 *Mathematics of Computation* is accessible from `www.ams.org/publications/`. Subscription prices for Volume 71 (2002) are as follows: for paper delivery, $388 list, $310 institutional member, $349 corporate member, $252 member of CBMS organizations; $233 individual member; for electronic delivery, $349 list, $279 institutional member, $314 corporate member, $227 member of CBMS organizations, $209 individual member. Upon request, subscribers to paper delivery of this journal are also entitled to receive electronic delivery. If ordering the paper version, add $12 for surface delivery outside the United States and India; $18 to India. Expedited delivery to destinations in North America is $17; elsewhere $56.

Back number information. For back issues see the `www.ams.org/bookstore`.

Subscriptions and orders should be addressed to the American Mathematical Society, P.O. Box 845904, Boston, MA 02284-5904 USA. *All orders must be accompanied by payment.* Other correspondence should be addressed to 201 Charles Street, Providence, RI 02904-2294 USA.

Copying and reprinting. Material in this journal may be reproduced by any means for educational and scientific purposes without fee or permission with the exception of reproduction by services that collect fees for delivery of documents and provided that the customary acknowledgment of the source is given. This consent does not extend to other kinds of copying for general distribution, for advertising or promotional purposes, or for resale. Requests for permission for commercial use of material should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA. Requests can also be made by e-mail to `reprint-permission@ams.org`.

Excluded from these provisions is material in articles for which the author holds copyright. In such cases, requests for permission to use or reprint should be addressed directly to the author(s). (Copyright ownership is indicated in the notice in the lower right-hand corner of the first page of each article.)

Mathematics of Computation is published quarterly by the American Mathematical Society at 201 Charles Street, Providence, RI 02904-2294 USA. Periodicals postage is paid at Providence, Rhode Island. Postmaster: Send address changes to Mathematics of Computation, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA.

© 2002 by the American Mathematical Society. All rights reserved.

This journal is indexed in *Mathematical Reviews*, *Zentralblatt MATH*, *Science Citation Index®*, *Science Citation Index™-Expanded*, *ISI Alerting Services℠*, *CompuMath Citation Index®*, and *Current Contents®/Physical, Chemical & Earth Sciences*.

♾ The paper used in this book is acid-free and falls within the guidelines established to ensure permanence and durability.

10 9 8 7 6 5 4 3 2 1 07 06 05 04 03 02

MATHEMATICS OF COMPUTATION

CONTENTS

Vol. 71, No. 237 January 2002

Patrice Coorevits, Patrick Hild, Khalid Lhalouani, and Taoufik Sassi, Mixed finite element methods for unilateral problems: convergence analysis and numerical studies 1

Weinan E and Jian-Guo Liu, Projection method III: Spatial discretization on the staggered grid 27

Samuel Albert, Bernardo Cockburn, Donald A. French, and Todd E. Peterson, A posteriori error estimates for general numerical methods for Hamilton-Jacobi equations. Part I: The steady state case 49

Jerry Markman and I. Norman Katz, Convergence of an iterative algorithm for solving Hamilton-Jacobi type equations 77

Xue-Cheng Tai and Jinchao Xu, Global and uniform convergence of subspace correction methods for some convex optimization problems ... 105

C. González, A. Ostermann, C. Palencia, and M. Thalhammer, Backward Euler discretization of fully nonlinear parabolic problems ... 125

James H. Bramble, Joseph E. Pasciak, and Olaf Steinbach, On the stability of the L^2 projection in $H^1(\Omega)$ 147

Carsten Carstensen, Merging the Bramble-Pasciak-Steinbach and the Crouzeix-Thomée criterion for H^1-stability of the L^2-projection onto finite element spaces 157

Bin Han and Rong-Qing Jia, Quincunx fundamental refinable functions and quincunx biorthogonal wavelets 165

Klaus Neymeyr, A geometric theory for preconditioned inverse iteration applied to a subspace 197

Attahiru Sule Alfa, Jungong Xue, and Qiang Ye, Accurate computation of the smallest eigenvalue of a diagonally dominant M-matrix 217

Nataša Krejić and Zorana Lužanin, Newton-like method with modification of the right-hand-side vector 237

Yuri Levin and Adi Ben-Israel, Directional Newton methods in n variables 251

I. H. Sloan and A. V. Reztsov, Component-by-component construction of good lattice rules 263

Kai-Tai Fang, Chang-Xing Ma, and Peter Winker, Centered L_2-discrepancy of random sampling and Latin hypercube design, and construction of uniform designs 275

Hannes Leeb, Asymptotic properties of the spectral test, diaphony, and related quantities 297

Norman Gray, Automatic reduction of elliptic integrals using Carlson's relations 311

Louis-Sébastien Guimond and Jiří Patera, Proving the deterministic period breaking of linear congruential generators using two tile quasicrystals 319

Maria Isabel González Vasco and Igor E. Shparlinski, Security of the most significant bits of the Shamir message passing scheme 333

Timothy Kohl and Daniel R. Replogle, Computation of several cyclotomic Swan subgroups 343
W. R. Oudshoorn and M. van der Put, Lie symmetries and differential Galois groups of linear equations 349
Igor A. Semaev, Special prime numbers and discrete logs in finite prime fields 363
D. R. Stinson, Some baby-step giant-step algorithms for the low hamming weight discrete logarithm problem 379
S. D. Galbraith, S. M. Paulus, and N. P. Smart, Arithmetic on superelliptic curves 393
John Abbott, Sparse squares of polynomials 407
Anastasios Simalarides, Upper bounds for the prime divisors of Wendt's determinant 415
István Gaál and Michael Pohst, On the resolution of relative Thue equations 429
Chris K. Caldwell and Yves Gallot, On the primality of $n! \pm 1$ and $2 \times 3 \times 5 \times \cdots \times p \pm 1$ 441
Tony Forbes, Fifteen consecutive integers with exactly four prime factors 449
H. N. Mhaskar, F. J. Narcowich, and J. D. Ward, Corrigendum to "Spherical Marcinkiewicz-Zygmund inequalities and positive quadrature" 453

Vol. 71, No. 238 **April 2002**

Paul Castillo, Bernardo Cockburn, Dominik Schötzau, and Christoph Schwab, Optimal a priori error estimates for the *hp*-version of the local discontinuous Galerkin method for convection–diffusion problems 455
Walter Zulehner, Analysis of iterative methods for saddle point problems: a unified approach 479
Susanne C. Brenner, Convergence of the multigrid V-cycle algorithm for second-order boundary value problems without full elliptic regularity 507
Gerard R. Richter, On the stability of a family of finite element methods for hyperbolic problems 527
Alfredo Bermúdez and Rodolfo Rodríguez, Analysis of a finite element method for pressure/potential formulation of elastoacoustic spectral problems 537
Laurent Gosse, Localization effects and measure source terms in numerical schemes for balance laws 553
Nicolas Fournier and Sylvie Méléard, A stochastic particle numerical method for 3D Boltzmann equations without cutoff 583
Roswitha März and Antonio R. Rodríguez-Santiesteban, Analyzing the stability behaviour of solutions and their approximations in case of index-2 differential-algebraic systems 605

G. Everest, I. Gaál, K. György, and C. Röttger, On the spatial distribution of solutions of decomposable form equations 633
George Boros and Victor H. Moll, Landen transformations and the integration of rational functions 649
Robert Schaback and Holger Wendland, Inverse and saturation theorems for radial basis function interpolation 669
Leyla Daruis, Pablo González-Vera, and Olav Njåstad, Szegö quadrature formulas for certain Jacobi-type weight functions 683
Reiji Suda and Masayasu Takami, A fast spherical harmonics transform algorithm 703
David M. Hough, Asymptotic estimation of Gaussian quadrature error for a nonsingular integral in potential theory 717
Andreas Enge, Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time 729
Peter Dräxler and Klara Kögerler, An algorithm for finding all preprojective components of the Auslander-Reiten quiver 743
Manfred Göbel, Finite SAGBI bases for polynomial invariants of conjugates of alternating groups 761
Peter Borwein and Kevin G. Hare, Some computations on the spectra of Pisot and Salem numbers 767
Frank Emmerich, Average equidistribution and statistical independence properties of digital inversive pseudorandom numbers over parts of the period 781
Andreas Stein and Edlyn Teske, The parallelized Pollard kangaroo method in real quadratic function fields 793
Diane Meuser and Margaret Robinson, The Igusa local zeta functions of elliptic curves 815
Harvey Dubner and Yves Gallot, Distribution of generalized Fermat prime numbers 825
Harvey Dubner, Repunit R49081 is a probable prime 833
Andreas Stein and Edlyn Teske, Explicit bounds and heuristics on class numbers in hyperelliptic function fields 837
Joshua Holden, Comparison of algorithms to calculate quadratic irregularity of prime numbers 863
Myra B. Cohen, Charles J. Colbourn, Lee A. Ives, and Alan C. H. Ling, Kirkman triple systems of order 21 with nontrivial automorphism group 873
Andrew Granville and Carl Pomerance, Two contradictory conjectures concerning Carmichael numbers 883

Vol. 71, No. 239 **July 2002**

Douglas N. Arnold, Daniele Boffi, and Richard S. Falk, Approximation by quadrilateral finite elements 909

Ville Havu and Juhani Pitkäranta, Analysis of a bilinear finite element for shallow shells I: Approximation of inextensional deformations 923

Carsten Carstensen and Sören Bartels, Each averaging technique yields reliable a posteriori error control in FEM on unstructured grids. Part I: Low order conforming, nonconforming, and mixed FEM 945

Sören Bartels and Carsten Carstensen, Each averaging technique yields reliable a posteriori error control in FEM on unstructured grids. Part II: Higher order FEM 971

Vladimir Druskin and Shari Moskow, Three-point finite-difference schemes, Padé and the spectral Galerkin method. I. One-sided impedance approximation 995

Heinrich Freistühler and Christian Rohde, Numerical computation of viscous profiles for hyperbolic conservation laws 1021

V. Girault and L. R. Scott, Hermite interpolation of nonsmooth functions preserving boundary conditions 1043

Donald J. Estep and Andrew M. Stuart, The dynamical behavior of the discontinuous Galerkin method and related difference schemes 1075

Xue-Cheng Tai and Paul Tseng, Convergence rate analysis of an asynchronous space decomposition method for convex minimization ... 1105

Pierre Dusart, Estimates of $\theta(x;k,l)$ for large values of x 1137

M. C. De Bonis, B. Della Vecchia, and G. Mastroianni, Approximation of the Hilbert transform on the real line using Hermite zeros 1169

Beatrice Meini, Efficient computation of the extreme solutions of $X + A^*X^{-1}A = Q$ and $X - A^*X^{-1}A = Q$ 1189

David W. Boyd, On a problem of Byrnes concerning polynomials with restricted coefficients, II 1205

Andreas Enge and Andreas Stein, Smooth ideals in hyperelliptic function fields 1219

Karl Entacher, Thomas Schell, and Andreas Uhl, Efficient lattice assessment for LCG and GLP parameter searches 1231

Hyun Kwang Kim and Jung Soo Kim, Evaluation of zeta function of the simplest cubic field at negative odd integers 1243

D. W. Farmer and K. James, The irreducibility of some level 1 Hecke polynomials 1263

Jesse Ira Deutsch, A computational approach to Hilbert modular group fixed points 1271

Keith Matthews, Thue's theorem and the diophantine equation $x^2 - Dy^2 = \pm N$ 1281

Denis Simon, Solving norm equations in relative number fields using S-units 1287

A. Paszkiewicz and A. Schinzel, On the least prime primitive root modulo a prime 1307

H. Dubner, T. Forbes, N. Lygeros, M. Mizony, H. Nelson, and P. Zimmermann, Ten consecutive primes in arithmetic progression 1323

Reviews and Descriptions of Tables and Books 1329
Heinz-Otto Kreiss and Hedwig Ulmer Busenhart **1**, Ronald A. Devore, Arieh Iserles, and Endre Süli, Editors **2**, Zhaojun Bai, James Demmel, Jack Dongarra, Axel Ruhe, and Henk van der Vorst, Editors **3**, Guillermo Sapiro **4**, Chee Keng Yap **5**, Kwok-Yan Lam, Igor Shparlinski, Huaxiong Wang, and Chaoping Xing, Editors **6**

Table Errata 1335
I. S. Gradshteyn and I. M. Ryzhik **636**, I. S. Gradshteyn and I. M. Ryzhik **637**

Toshihiro Kumada, Hannes Leeb, Yoshiharu Kurita, and Makoto Matsumoto, Corrigenda to "New primitive t-nomials ($t = 3, 5$) over $GF(2)$ whose degree is a Mersenne exponent," and some new primitive pentanomials 1337

Vol. 71, No. 240 **October 2002**

Ivo Babuška and Jan Chleboun, Effects of uncertainties in the domain on the solution of Neumann boundary value problems in two spatial dimensions 1339

Christine Bernardi and Frédéric Hecht, Error indicators for the mortar finite element discretization of the Laplace equation 1371

Ricardo H. Nochetto and Lars B. Wahlbin, Positivity preserving finite element approximation 1405

Zhimin Zhang, Derivative superconvergent points in finite element solutions of harmonic functions—A theoretical justification 1421

Ulisse Stefanelli, Analysis of a variable time-step discretization of the three-dimensional Frémond model for shape memory alloys 1431

Gabriel N. Gatica and Norbert Heuer, Conjugate gradient method for dual-dual mixed formulations 1455

Tai-Lin Wang and William B. Gragg, Convergence of the shifted QR algorithm for unitary Hessenberg matrices 1473

Johnson C. M. Fok, Benyu Guo, and Tao Tang, Combined Hermite spectral-finite difference method for the Fokker-Planck equation 1497

M. P. Calvo and C. Palencia, Avoiding the order reduction of Runge-Kutta methods for linear initial boundary value problems 1529

Nikolai Bakaev and Alexander Ostermann, Long-term stability of variable stepsize approximations of semigroups 1545

Avram Sidi, New convergence results on the generalized Richardson extrapolation process GREP$^{(1)}$ for logarithmic sequences 1569

Winfried Kohnen and Michael Kuß, Some numerical computations concerning spinor zeta functions in genus 2 at the central point 1597

I. H. Sloan, F. Y. Kuo, and S. Joe, On the step-by-step construction of quasi–Monte Carlo integration rules that achieve strong tractability error bounds in weighted Sobolev spaces 1609

Fred J. Hickernell and Xiaoqun Wang, The error bounds and tractability of quasi–Monte Carlo algorithms in infinite dimension 1641

Shuhong Gao and Alan G. B. Lauder, Hensel lifting and bivariate polynomial factorisation over finite fields 1663
Joachim von zur Gathen and Jürgen Gerhard, Polynomial factorization over $\mathbb{F}_2$ 1677
Zhenxiang Zhang, A one-parameter quadratic-base version of the Baillie-PSW probable prime test 1699
Stéphane Louboutin, Computation of class numbers of quadratic number fields 1735
Ana-Cecilia de la Maza, Bounds for the smallest norm in an ideal class ... 1745
A. Campillo and J. I. Farrán, Symbolic Hamburger-Noether expressions of plane curves and applications to AG codes 1759
A. Paszkiewicz and A. Schinzel, Numerical calculation of the density of prime numbers with a given least primitive root 1781
Reviews and Descriptions of Tables and Books 1799
R. B. Pari and D. Kaminski **7**
Table Errata 1801
M. Abramowitz and I. Stegun **638**
John B. Friedlander, Carl Pomerance, and Igor E. Shparlinski, Corrigendum to "Period of the power generator and small values of Carmichael's function" 1803